

IN THE CLAIMS

The following listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims

- B1
1. (currently amended) A system for enabling the preparation, execution and secure management of an electronic chattel paper agreement comprising:
- a server processing unit and a server memory device electrically coupled to the server processing unit;
 - a client processing unit and a client memory device electrically coupled to the client processing unit;
 - a server program module, stored in the server memory device, for providing instructions to the server processing unit,
 - a client program module, stored in the client memory device, for providing instructions to the client processing unit, and
 - a communication medium, communicatively coupling the server processing unit and the client processing unit;
- the client processing unit, responsive to the instructions of the client program module and the server processing unit, responsive to the instructions of the server program module, being operative to:
- authorize access to the system;
 - generate at least one unexecuted electronic chattel paper document;
 - prevent the creation of fraudulent versions of the electronic chattel paper document;

allow electronic signatures electrically input by parties to a chattel paper transaction to be associated with the electronic document thereby generating an electronic chattel paper agreement; and

maintain an authoritative copy of the electronic chattel paper agreement in the server memory device of the server processing unit.

B1
2. (original) The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are being operative to authorize access to the system by:

the client processing unit

receiving access information from the input device,

transmitting the access information to the server processing unit over the communication medium, and

receiving an authorized indicator from the server processing unit over the communications medium; and

the server processing unit

receiving the access information from the client processing unit over the communications medium,

verifying that the access information qualifies for granting access to the system, and

transmitting an authorized indicator to the client processing unit over the communications medium.

3. (currently amended) The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and where in the client processing unit and the server processing unit are operative to generate at least one electronic chattel paper document by:

the client processing unit

receiving pertinent information from the input device, and

integrating the pertinent information into an electronic template.

4. (currently amended) The system of claim 3, wherein the electronic template includes predefined chattel paper document information and a predefined chattel paper document format, and the client processing unit and the server processing unit are operative to integrate the pertinent information into the electronic template by:

receiving a complete indicator from the input device, the complete indicator indicating that no additional pertinent information will be received by the client processing unit, and

merging the pertinent information and the predefined document information to generate the electronic chattel paper document conforming to the predefined chattel paper document format.

5. (currently amended) The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and where the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the

electronic chattel paper document by the client processing unit, in response to generating the electronic chattel paper document, rejecting any attempts to modify the electronic document.

6. (currently amended) The system of claim 1, further comprising an input device electrically coupled to the client processing unit; and wherein the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the chattel paper electronic document by the client processing unit, in response to generating the electronic chattel paper document, encrypting the electronic chattel paper document and generating a signature key based at least in part on the contents of the electronic chattel paper document.

7. (currently amended) The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and the client processing unit and the server processing unit are operative to prevent the creation of fraudulent versions of the electronic chattel paper document by:

the client processing unit,

in response to generating the electronic chattel paper document,
encrypting the electronic chattel paper document, and

in response to an attempt to modify the electronic chattel paper
document, rendering the electronic chattel paper document invalid.

8. (currently amended) The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and wherein the client processing unit and the server processing unit are operative to allow electronic signatures electronically input by parties

to the chattel paper transaction to be associated with the electronic chattel paper document thereby generating an electronic agreement by:

the client processing unit

receiving at least one signature input from the input device,

creating a signature file containing the signature input, and

encrypting the signature file using an encryption key that is

based at least in part on the contents of the electronic chattel paper document.

9. (currently amended) The system of claim 1, further comprising an input device electrically coupled to the client processing unit, and the client processing unit and the server processing unit are operative to maintain an authoritative copy of the electronic chattel paper agreement in the server memory device of the server processing unit by:

the client processing unit

receiving a submit indicator from the input device, and in response to receiving the submit indicator, transmitting the electronic chattel paper agreement and the electronic electronically input signatures associated with the electronic chattel paper agreement to the server processing unit over the communications medium; and

the server processing unit

receiving the electronic chattel paper agreement and the electronic electronically input signatures,

preventing any modifications to the electronic chattel paper agreement and the signature file, and

providing an unauthorized copy indicator on any electronic and hard copies of the ~~electronic~~ chattel paper agreement, the unauthorized copy indicator indicating that the electronic and hard copies of the electronic chattel paper agreement are not the authoritative copy of the electronic chattel paper agreement.

10. (currently amended) A method for creating an electronic chattel paper agreement and maintaining an authoritative copy of the electronic chattel paper agreement, the method comprising ~~the steps of~~:

(a) receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic chattel paper document;

(b) in response to receiving a complete indicator from the input source, the complete indicator indicating that the received subset of input information is complete, generating an electronic chattel paper document by merging the subset of input information with a chattel paper document template;

(c) electronically receiving a set of ~~electronic~~ signatures by parties to a chattel paper transaction from the input source, whereby upon receiving the set of ~~electronic~~ chattel paper signatures, the electronic chattel paper document is considered an electronic chattel paper agreement; and

(d) in response to receiving a submit indicator, storing the electronic chattel paper agreement within an access restricted computer system, the stored electronic chattel paper agreement constituting an authoritative copy of the electronic chattel paper agreement.

11. (currently amended) The method of claim 10, further comprising after the generating the electronic chattel paper document ~~step, the step of~~ providing a signature indicator to the input source, the signature indicator indicating that the generating step is complete and that the electronic chattel paper document requires the electronic input of the set of ~~electronic~~ signatures.

12. (currently amended) The method of claim 11, further comprising prior to the receiving a set of signatures ~~step, the step of~~ encrypting the electronic chattel paper document.

13. (currently amended) The method of claim 12, further comprising after the encrypting ~~step, the step of~~ preventing the electronic chattel paper document from being modified.

14. (currently amended) The method of claim 10, further comprising prior to the storing ~~step, the step of~~ encrypting the set of ~~electronic~~ electronically input signatures using an encryption key, the encryption key being based at least in part, on the contents of the electronic chattel paper document, whereby if the contents of the electronic chattel paper document are modified, the ~~electronic~~ electronically input signatures and the electronic chattel paper agreement will be invalid.

15. (currently amended) The method of claim 10, further comprising prior to the storing ~~step, the step of~~ providing an indicator that the set of ~~electronic~~ electronically input signatures has been received and that the electronic chattel paper agreement is complete.

16 (currently available) In a distributed computer system including at least one server device and at least one client device communicatively coupled to the server device, a method for maintaining an authoritative copy of an electronic chattel paper agreement, the method comprising the steps of:

B1 (a) a client device receiving a set of input information from an input source, the set of input information including a subset of information necessary to generate an electronic chattel paper document and a set of signatures necessary to make the electronic chattel paper document a binding chattel paper agreement;

(b) the client device encrypting the electronic chattel paper document using a first key and the set of signatures using a second key, the second key being based at least in part on the contents of the electronic chattel paper document, whereby any modifications to the electronic chattel paper document would result in invalidating the set of signatures;

(c) the client device transferring the encrypted electronic chattel paper document and the encrypted set of signatures to a server device over a communications medium, the server device being access restricted, the stored electronic chattel paper document and set of signatures constituting the only authoritative copy of the electronic chattel paper agreement.

17. (currently amended) A client system operating within an electronic chattel paper document system, the electronic chattel paper document system including a server, a server memory storage device and a server program module, the client system comprising:

a client processing unit;

a client memory device, a display device and an input device all electrically coupled to the client processing unit; a client program module, stored in the client memory device, for providing instructions to the client processing unit;

a communication medium, communicatively coupling the client system to the electronic document system; and

the client processing unit, responsive to the instructions of the client program module, being operative to:

authorize access to the electronic chattel paper document system by

receiving access information from the input device,

transmitting the access information to the server over the communication medium, and

receiving an authorization indicator from the server processing unit over the communications medium;

generate at least one electronic chattel paper document;

prevent the creation of fraudulent versions of the electronic chattel paper document;

allow electronic electronically input signatures to be associated with the electronic chattel paper document, thereby generating an electronic chattel paper agreement,

receiving a set of signatures from the input device,

creating at least one signature file containing the set of signatures, and

encrypting the signature file using an encryption key that is based at least in part on the contents of the electronic chattel paper document; and

transfer the electronic chattel paper document and the encrypted signature file as an electronic chattel paper agreement to the server over the communications medium.

18. (currently amended) The client system of claim 17, wherein the client processing unit is operative to generate at least one electronic chattel paper document by:

receiving pertinent information from the input device; and

merging the pertinent information with predefined chattel paper document information to generate an electronic chattel paper document conforming to a predefined chattel paper document format.

19. (currently amended) The client system of claim 17, wherein the client processing unit is operative to prevent the creation of fraudulent versions of the electronic chattel paper document by, after generating the electronic chattel paper document, encrypting the electronic chattel paper document and rejecting any attempts to enter additional pertinent information.

20. (currently amended) The system of claim 17, wherein the client processing unit is operative to prevent the creation of fraudulent versions of the electronic chattel paper document by:

detecting an attempt to modify the electronic chattel paper document, and

in response to detecting an attempt, rendering the electronic chattel paper document invalid.
